WISCONSIN

Office of Privacy Protection

Safeguarding Information for Your Future

Protecting Your Computer from Hackers

In today's day and age, we use computers for everything. We store pictures and music on computers. We keep in touch with friends and family by using e-mail. We pay our bills online. We do our banking online. We do our shopping online. We apply for jobs online.

BUT….what happens when your computer is hacked? Here are some simple, yet very important steps you can take to help prevent hackers from taking over your computer and personal information.

- **Back up your information often.** You can save your computer data to a CD, DVD, external hard drive or a memory stick. That way, if your computer ever crashes or is hacked, you will not lose all of your information.

- **Update your operating system regularly**. Computer operating systems are periodically updated to stay up to date with technology requirements and to fix weak spots that may be targeted by hackers. Be sure to install the updates to make sure your computer has the latest protection.

- **Use strong passwords and change them often.** By using a password that is greater than eight characters in length, you reduce the chance that someone will guess your password. Use passwords that contain upper and lower case letters, numbers, and punctuation. Change your password every three months and do not reuse passwords. This is especially true for passwords that are used to access your email and bank accounts.

- **Do not click on pop-ups.** Pop-up windows on the internet are quick advertising tools, but beware of "too good to be true" offers. Not only can these pop-ups slow your computer and internet speed down, but by clicking on these you can accidentally be signed up for unauthorized services. Turn your browser's information bar to not allow pop-ups.

- **Be careful what you download.** Some of the most destructive viruses have been hidden in internet programs and applications or e-mail attachments. Be sure you download from a trusted source. As for e-mails, never click on links or attachments if you do not recognize the sender. Even if you do know the sender, beware! Because it is possible their computer was hacked and is sending out infected e-mails.

- **Do not send sensitive or private information via email.** Email is not usually encrypted, or in other words not in a "secret code," and can be intercepted and read by hackers. However, encryption software packages are available.

Department of Agriculture, Trade and Consumer Protection
2811 Agriculture Drive, PO Box 8911, Madison, WI 53708-8911
(608) 224-5163 • (800) 422-7128 • Fax: (608) 224-4677 • www.privacy.wi.gov

- **Use antivirus software and set it to update itself daily.** There are many commercial products that can help you protect your computer from various viruses. Most virus protection software has a feature that will scan downloaded files automatically and some will even scan incoming emails by default.

- **Avoid installing unnecessary, unfamiliar, or untested software.** This could include games, toolbars or screensavers that could leave your computer open to attacks. Spyware and viruses are often downloaded by installing unfamiliar programs.

- **Use a personal firewall.** A firewall acts as a barrier between you and the internet. It helps keep hackers out and helps prevents malicious software from sending your personal information to criminals. There are free and retail versions available and firewalls can come in the form of both software and hardware.

- **Be careful of wireless networks.** For your home network, change your wireless router's default password. Enable WPA encryption and use a long password or passphrase. If WPA encryption is not available, WEP encryption is better than nothing. For public wireless access (such as at restaurants, libraries or cafes), be aware if the network is unsecured. Cyber criminals like to use these networks to hack into your computer and steal your personal data.

- **Turn your computer off when not in use.** Leaving your computer on and unattended could leave it open for an attack by hackers. Protect your computer, and save energy, by turning your computer off when you are not using it.

We may not be able to prevent all hacking, but we can help equip consumers with the tools and knowledge to protect themselves from cyber criminals.

"I've been hacked!"
Steps to Recover From a Computer Attack

Here are tips we recommend people take if their e-mail accounts or social networking accounts have been hacked.

- **If you can access your compromised account, let your contacts know you have been hacked.** Some scams target the family and friends in your e-mail contact list. The scammers make it sound like you are in a foreign country and need money wired to you right away. In order to help make sure your family and friends do not wire money to these criminals, e-mail your contacts and let them know your account has been hacked. Let them know they should watch out for suspicious e-mails claiming to be from you.
- **If you cannot get into your compromised account, contact the e-mail or social network provider and ask that the account be shut down.** Many sites will walk you through how to report a hacked account, or how to deactivate/delete a hacked account. Each site varies, but you should start by clicking on the site's "Help" link, and look up how to close down your account. If you cannot find what you are looking for, e-mail the site's help center.
- **Change all of your usernames and passwords.** Especially if you use the same username and password for all of your online accounts. If the hackers have one correct username and password, and the hackers were able to monitor your internet activity and which websites you visited, they may try to log onto your other sites (such as banking, utility or networking).

- **If your e-mail account was compromised, be sure to remove all information before you deactivate or delete it.** You never know if the hackers will keep going back to your account and using it to get to your contacts. Or sometimes you may have saved e-mails that list private information such as account information, birth date, or even social security numbers. If you can still access your account, be sure to delete all of your contacts and all of your saved e-mails. This will help minimize the information the hackers can find out about you.
- **If you create a new account, be sure to:**
    - E-mail your old contacts with your new account information. Explain that your old account was compromised and that they shouldn't trust any e-mails or messages that come from your old e-mail account.
    - Update any paperless billing statements that you receive via e-mail. You don't want to miss any payments because your statement goes to an old account. Make sure you update your online account information so that all billing statements now go to your new e-mail address.

Technology continues to change and evolve. It is what keeps us connected with loved ones, sharing photos with friends and even paying our bills on time. Unfortunately, hackers are also continuously changing and evolving…so that they might continue to prey off of our vulnerability. We may not be able to prevent all hacking, but we can help equip consumers with the tools and knowledge to protect themselves from cyber criminals.

If your computer has been hacked into and you feel your safety is in jeopardy, or think that the hacker is someone you know, you should call your local police.

For more information or to file a complaint, visit our website or contact the Office of Privacy Protection.

Office of Privacy Protection
Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911

E-MAIL:
DATCPWisconsinPrivacy@wisconsin.gov
WEBSITE: www.privacy.wi.gov

Toll-free in WI: (800) 422-7128
(608) 224-5163
FAX: (608) 224-4677
TTY: (608) 224-5058